

Docket No.: M4065.0486/P486  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Doug Rollins

Application No.: 09/993,495

Confirmation No.: 8165

Filed: November 27, 2001

Art Unit: 2137

For: METHOD AND APPARATUS FOR WEP KEY  
MANAGEMENT AND PROPAGATION IN A  
WIRELESS SYSTEM

Examiner: S. Gelagay

**DECLARATION OF DOUG ROLLINS UNDER 37 CFR 1.131**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

I, Doug Rollins, declare and state as follows:

1. I reside in Nampa, Idaho and have a mailing address of 7626 Cypress Ln, Nampa, Idaho, 83687.
2. I am presently employed as Director of Research and Development for MPC Computers, LLC. At the time this invention was conceived, MPC Computers LLC was known as MicronPC and was a subsidiary of Micron Technology, Inc. ("Micron").
3. I am the sole inventor of U.S. Patent Application 09/994,495 (the "495 application"), filed on November 21, 2001.

DSMDB-2517702

4. I have reviewed and I understand the '495 application, including the currently pending claims (the "Claimed Invention").

5. The '495 application is assigned to Micron Technology, Inc., as evidenced by a copy of the attached assignment (Exhibit A).

6. I conceived the subject matter of the Claimed Invention prior to October 24, 2001, as evidenced by the Micron Technology, Inc. Invention Disclosure (Exhibit B), which is a copy of the invention disclosure forwarded to the law firm of Dickstein Shapiro LLP ("Dickstein"). The actual date on this document has been redacted, as has any description and/or material not relevant to the conception of the Claimed Invention; however, the date of the Disclosure is prior to October 24, 2001.

7. An attorney at Dickstein drafted a Memorandum summarizing my invention and listing a number of questions regarding the invention (Exhibit C). The Memorandum has been redacted to remove some privileged matter. Although the date of the Memorandum has been redacted, it is prior to October 24, 2001.

8. I received a first draft of the '495 patent application (Exhibit D) from Dickstein through Stacy Summers, a Patent Assistant at Micron, with a cover letter (Exhibit E) on October 22, 2001. The letter has been redacted to remove privileged and non-relevant matter.

9. It can be seen at least from the Figures and description on pages 1-3 and 7-8 of the Invention Disclosure (Exhibit B) as well as Paragraphs [0013], [0026], [0027] and [0029] of the first draft of the '495 application (Exhibit D) that I conceived the idea of at least "physically separating from said wireless station a network communications device; physically connecting

said separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; [and] physically reconnecting said network communications device containing said new encryption key with said wireless station of said network," as recited by the current claim 1 prior to October 24, 2001.

10. The description and figures found on at least pages 1-3 and 7-8 of the Invention Disclosure (Exhibit B) as well as in Paragraphs [0006], [0013], [0021], [0026], [0027] and [0029] of the first draft of the '495 application (Exhibit D) additionally shows that I conceived of the subject matter of current independent claims 8, 15, 17 and 20 prior to October 24, 2001.

11. After thoroughly reviewing the draft as time allotted due to other pressing business matters, I found it to be acceptable to me. Stacy Summers, the Patent Assistant at Micron, requested signature papers by e-mail (Exhibit E) from Dickstein on November 1, 2001.

12. Signature papers were forwarded to me along with a final draft of the '495 application from Dickstein through Stacy Summers, a Patent Assistant at Micron, with a cover letter (Exhibit F) on November 7, 2001

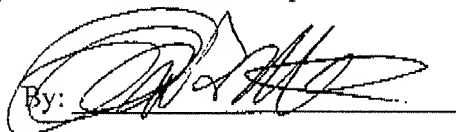
13. As time allotted due to other pressing business matters, I reviewed the final draft and forwarded the executed Declaration and Assignment (Exhibit B) to Dickstein through Stacy Summers, a Patent Assistant at Micron, by mail with a cover letter (Exhibit G) dated November 21, 2001, which was received by Dickstein on November 26, 2001, as shown by the stamp on the cover letter. The application was filed in the United States Patent and Trademark Office by

Dickstein on November 27, 2001.

14. As evidenced herein and by the attached Exhibits, the preparation of the '495 application covering the Claimed Invention was diligently pursued from prior to the reference date of October 24, 2001 to the filing date of November 27, 2001.

All statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the above-identified patent.

Date: 11/1/08

By: 

Doug Rollins

**EXHIBIT A**

For value received, I, Doug Rollins, hereby sell, assign and transfer to Micron Technology, Inc., a corporation of the State of Delaware, having an office at 8000 S. Federal Way, Boise, Idaho 83706-9632, U.S.A., and its successors, assigns and legal representatives, the entire right, title and interest, for the United States of America, in and to certain inventions related to an invention entitled METHOD AND APPARATUS FOR WEP KEY MANAGEMENT AND PROPAGATION IN A WIRELESS SYSTEM, described in an application for Letters Patent of the United States, executed by me of even date herewith, and all the rights and privileges in said application and under any and all Letters Patent that may be granted in the United States for said inventions; and I also concurrently hereby sell, assign and transfer to Micron Technology, Inc. the entire right, title and interest in and to said inventions for all countries foreign to the United States, including all rights of priority arising from the application aforesaid, and all the rights and privileges under any and all forms of protection, including Letters Patent, that may be granted in said countries foreign to the United States for said inventions.

I authorize Micron Technology, Inc. to make application for such protection in its own name and maintain such protection in any and all countries foreign to the United States, and to invoke and claim for any application for patent or other form of protection for said inventions, without further authorization from me, any and all benefits, including the right of priority provided by any and all treaties, conventions, or agreements.

I hereby consent that a copy of this assignment shall be deemed a full legal and formal equivalent of any document which may be required in any country in proof of the right of Micron Technology, Inc. to apply for patent or other form of protection for said inventions and to claim the aforesaid benefit of the right of priority.

I request that any and all patents for said inventions be issued to Micron Technology, Inc. in the United States and in all countries foreign to the United States, or to such nominees as Micron Technology, Inc. may designate.

1365357  
136535

mana  
the ne  
with th  
Admir

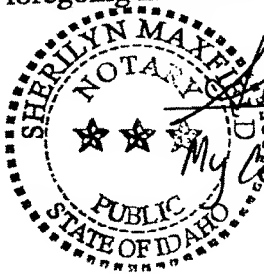
*Doug Rollins*

Doug Rollins

Date: 1/14/01

United States of America )  
State of Idaho ) ss.:  
County of Ada )

On this 14<sup>th</sup> day of November, 2001, before me  
personally came Doug Rollins, to me known to be the individual  
described in and who executed the foregoing instrument, and acknowledged execution  
of the same.



*Sherilyn Maxfield*  
Notary Public

*My Commission Expires: 10/22/03*

**EXHIBIT B**

MICRON ELECTRONICS

70-0586

**INVENTION DISCLOSURE FORM**

MICRON LEGAL

**1. INVENTOR(S)**

(a) Doug Rollins

~~01.00791~~  
MUEI-0586

**2. DESCRIPTION**

**2.1 Title of invention**

*Method and Apparatus for WEP key management and propagation in a wireless network management system.*

**2.2 What is the problem to be solved by your invention?**

Wireless networks depend on secret encryption keys for security. This encryption mechanism or "WEP" key (**W**ired **E**quivalency **P**rivacy) is well known and well documented in various IEEE standards and is implemented in commercially available network devices.

However, managing the private keys (and hence securing the network system) is cumbersome. It requires the network administrator to manually choose a new WEP key (the greatest security is generated by a random key), update every access point using that key and the Access Point management application, and then update every user's network device (such as a notebook PC) with the new key. To complicate this further, the WEP key is currently stored in the software associated with the card, not on the card itself. That is, to change the WEP key on a notebook PC, the Administrator must gain physical access to the notebook, start the Operating System, start the card's support application, and manually enter the WEP key.

If the key changes (and keys should be changed on a regular schedule) and the network devices (clients and access points) are not properly updated (clearly a possibility when the key value is entered by hand), the users with the old keys will lose connectivity. If the keys are not updated frequently, network security can suffer. Finally, if the keys are chosen by a human, randomness is not ensured and hence security can suffer.

My invention is a method and apparatus to manage and propagate quasi-random keys based on a schedule. My invention ensures that each and every access device is updated on this schedule and likewise ensures that all physically compromised (stolen) devices are unable to gain access to the network.

**2.3 How did others solve the problem prior to your invention (If known)? (Describe the**

**“prior art.”) Why are these solutions non-optimal? Provide copies of any known “prior art.”**

The current IEEE implementation of WEP requires the following steps to choose and update a key:

1. Network Administrator chooses a new key (either 40-bit or 128-bit as specified in the IEEE 802.11x standards.
2. Network Administrator propagates the new keys to the Access Points in the wireless network using Access Point vendor-supplied management applications (where available) or does so manually.
3. *Each network card* that is to have access to the wireless network has its WEP keys updated *manually* inside the Operating System. A Technician uses the local management application (an application loaded on the network access device or PC) to type in the new WEP keys.
4. This process is repeated *every time* the WEP keys are changed.

This process is well known and well documented.

This solution is non-optimal for several reasons:

1. Since it is cumbersome and manual, it does not encourage Network Administrators to change their WEP keys regularly.
2. If the keys are not changed and a network access device (notebook PC with a PC Card) is compromised, the network security is compromised.
3. There is not *inherent* schedule mechanism for key management.

**2.4 Provide a hardware block diagram of your invention. Also, describe how the hardware components of your invention are coupled together. Please include an assembly drawing if it is available. (If your invention is a pure software invention, then disregard this question.)**

Hardware block diagram attached. Diagram shows WEP key propagation through Ethernet to each WEP-enabled device on the network.

Management/WEP Key Generation system is connected to a conventional Ethernet network

Access Points shown are bridges between the Ethernet network and the wireless network. These devices are well known and documented.

Wireless NICs are PC-Card wireless network cards that plug into the PC Card Tray. This tray is also attached to the Ethernet network. This tray has several PC Card slots into which a wireless PC Card is inserted for WEP key updating. The tray is powered.

**2.5 Provide a flow chart of the steps performed by your invention. Also, describe how your invention operates.**



Flowchart attached.

1. Management Station generates new random WEP key according to network implementation (40-bit or 128-bit).
2. New key is checked against used keys (i.e. has this key been used before). The number of used keys against which the new key is compared is set by the Network Administrator (a key reuse interval). If the new has been used within this interval it is discarded and a new key is generated. This cycle repeats until a new key is generated.
3. Once a good key (that is, a key that has not already been used within the user-specified interval) is generated, the Management Station checks the user-defined key propagation schedule. If a new key is not yet needed, it is stored on the Management Station and a delay loop executes until the next scheduled key propagation.
4. If the key update schedule specifies a new key should be propagated, the key is propagated to all WEP-enabled devices.
5. For each device discovered, the Management Station determines if the device is an Access Point or a PC Card Tray.
6. If the device is an Access Point, the AP's WEP key is updated and the system then seeks to update the next WEP-enabled devices.
7. If the device is a PC Card Tray, the WEP key of the card in the first slot is updated *regardless of the current key value*. This process repeats until all the cards in the given tray have the new WEP key. The tray reports back to the Management Station that the all cards in the tray have been updated. This process operates in parallel for all PC Card Trays (and hence all PC Cards).
8. When a user requires access to the wireless network, the Administrator removes a wireless NIC from the PC Card Tray and issues that key to the user. Since the card was removed from the tray and since the WEP keys have propagated across the network, neither the user nor the Administrator needs to enter the new WEP key. The user has instant access.

## **2.6 Describe the advantages of your invention.**

My invention is an improvement over the current WEP key management system in the following ways:

1. Current WEP key management systems are cumbersome and completely manual. My invention automates this function.
2. My invention ensures the user of random WEP keys.
3. My invention encourages the Network Administrator to change keys frequently, thus increasing security.
4. Since the new WEP keys are automatically propagated, there is no chance for user error when entering the new key. This drives support costs down significantly.

- 5 My invention is scalable; it can support as many or as few wireless devices to which it has access (on the same subnet – this is a limitation of TCP/IP). If there are other devices on other subnets, there are well known methods to permit the Management Station access to the devices on the other subnets.

### **3. CONCEPTION OF INVENTION**

- 3.1 Identify the date when you first conceived the invention. (If not sure, give the earliest date of which you are sure.)

030101

- 3.2 To whom was the idea first described and on what date? (Other than a co-inventor.)

Steve Price, co-worker

- 3.3 Identify the date of the first tangible record such as computer simulation, tape out, drawing or written description. Please specify type and location.

030701. This document.

- 3.4 Identify related invention disclosures or related patents. Attach copies, if available.

None of which I am aware. The IEEE 802.11x standard discusses WEP keys, but not their management. The specification is available from [www.ieee.org](http://www.ieee.org)

### **3.5 IMPORTANT DATES**

- a. Has the invention been disclosed outside the company?

No

If yes, to whom, when, and in what form?

N/A

- b. Have any articles describing your invention been published?

None of which I am aware.

If yes, list author (s), title of article, publication and date.

- c. Have any engineering samples been given out?

None of which I am aware.

If yes, to whom and on what date?

N/A

d Has any product using the invention been sold or offered for sale?

*None of which I am aware*

If yes, to whom and on what date?

N/A

e Has any product that has been sold or offered for sale been manufactured or tested using the invention?

*None of which I am aware.*

If yes, to whom and on what date?

N/A

**3.6 When will (or did) Micron begin use of the invention experimentally?**

*Unknown*

**3.7 When will (or did) Micron begin production of or use of this invention?**

*Unknown*

**3.8 Was the invention developed during a joint development agreement or other contract with an outside company or the U.S. Government? If so, please explain.**

*No*

4. INVENTOR (S):

Name: Doug Rollins User Name: dlrollins  
Micron Phone: (208) 898-3034 Fax: 898-2183 e-mail: Dlrollins@micronpc.com

Employee #: 16064 Company #: 12 Dept. #: 3500


Dept Name: Product and Brand Marketing

Company: ☒ MEI/Nampa/PC Design and Manufacture  
☐ MEI Other \_\_\_\_\_  
☐ SpecTek \_\_\_\_\_

Home Address: 7626 Cypress Lane  
Nampa ID 83687

County: USA Citizenship: USA


Inventor's Supervisor: Tina Wright

Inventor Signature:  Date: 03-06-01

\*If more than one inventor, attach additional copies of this section, one for each inventor

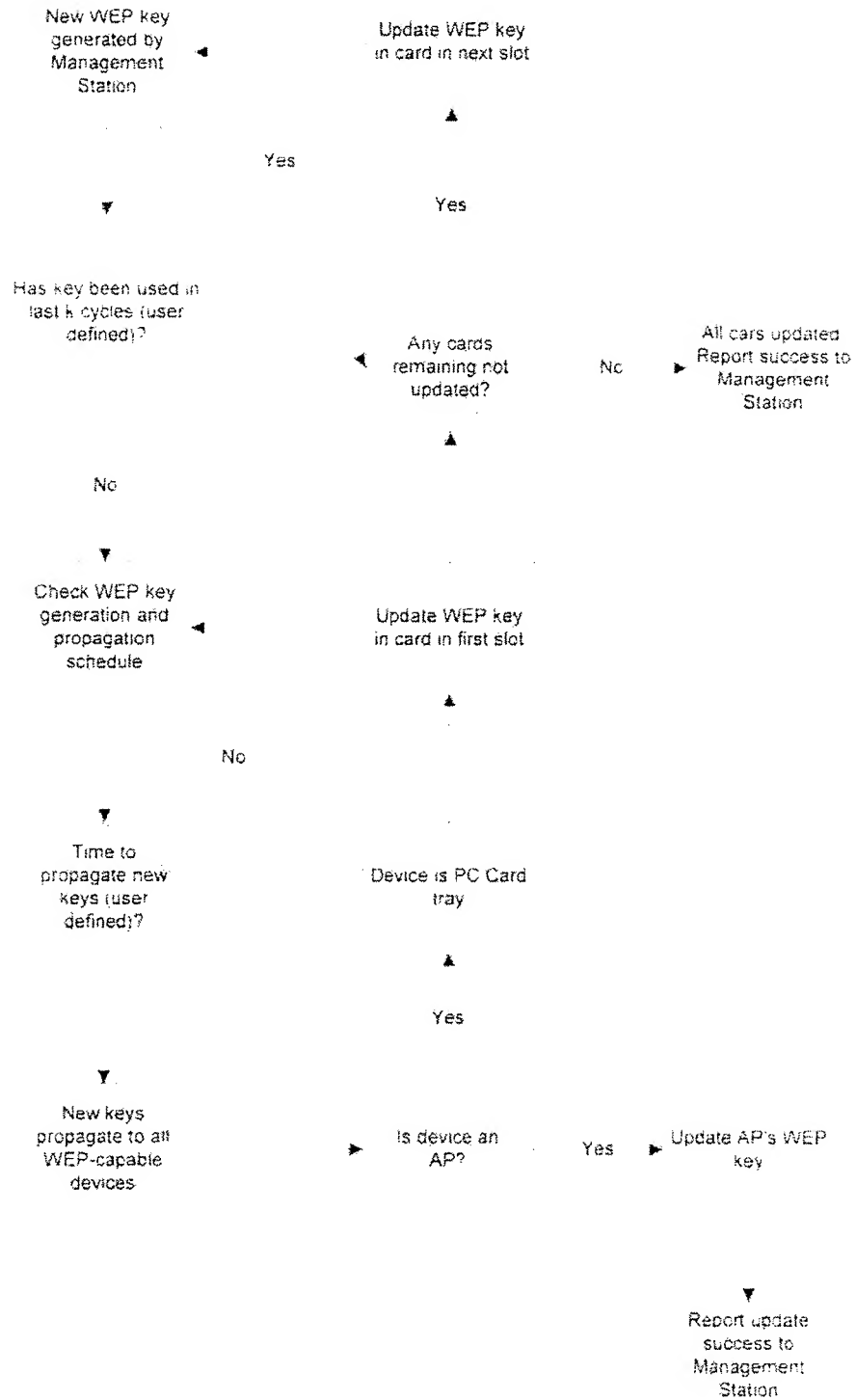
5. WITNESS (required for a single inventor)

If there is only one inventor, a witness should sign and date this disclosure. A witness in this case is a non-inventor who understands the nature of the invention.

  
(Signature of Witness)  
Dease Allen  
(Printed Name of Witness)  
3-7-01  
(Date)

Note If you have any questions or wish assistance completing this form, please call the  
Legal/Patent Department. (208) 898-1316 or 4792.

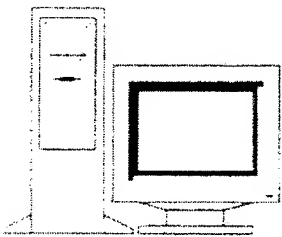
## WEP key update sequence (across network)



Network connections and WEP key propagation

WEP keys are algorithmically generated on Management/WEP Key Generation Station

Schedule propagates keys to all known WEP capable devices through Ethernet



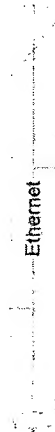
Management/WEP Key Generation Station



Access Point



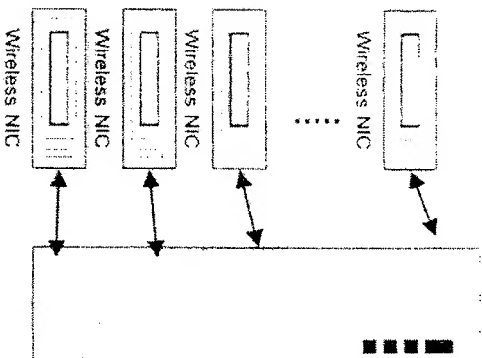
Access Point



Ethernet



Access Point



PC Card Tray

PC Card tray holds wireless NICs WEP keys are propagated to each wireless NIC in tray

# EXHIBIT C

## MEMORANDUM

TO: Tom D'Amico

FROM: Adam Kaplan

DATE: [REDACTED]

RE: M4065.0486 (70-0586) Method and Apparatus for WEP Key  
Management and Propagation in a Wireless System  
Doug Rollins

CONTAINS PROPRIETARY AND  
CONFIDENTIAL COMMERCIAL  
INFORMATION NOT TO BE RELEASED

---

The invention teaches a simplified method of updating encryption keys in a wireless network implementing the IEEE 802.11 protocol Wired Equivalency Privacy ("WEP"). The prior art [REDACTED]

[REDACTED] do not teach the steps of the present invention.

The present invention is for a network that is run over an ethernet with PCs connected to the network over wireless Network Interface Cards ("NIC"). WEP keys are used to encrypt the messages sent to and from PCs to avoid eavesdropping. A

management station generates a new random WEP key. The new WEP key is checked against a list of recently used keys to insure that a key is not used more than once in a administrator-defined length of time. If the new WEP key matches one of the recently used keys, a new one is generated and the process is repeated.

Once a key that does not match any recently used keys is generated, the management station checks the user-defined key propagation schedule. If a new key is not needed yet, it is stored on the management station and a delay loop executes until the next scheduled key propagation.

Once the key update schedule indicates that a new key should be propagated, the key is propagated to all WEP-enabled devices. WEP-enabled devices are connected to the management station by physical connections through an ethernet. Where a network administrator used to be required to enter a new WEP key manually into each PC, in the present invention, a new WEP key is propagated to PC card trays and Access Points ("AP"). Network Interface Cards ("NIC") are inserted into the PC card trays and their WEP keys are updated. This eliminates the necessity of manually entering the WEP key into every computer. Instead, each NIC is inserted into a PC card tray and the WEP key is updated. In addition to updating PC card trays, APs are updated. (see questions below, what an access point is is unclear in the disclosure).

#### Questions:

1. What happens when a NIC is placed in a PC card tray after the WEP key generation station has updated the cards in the PC card tray? Is it automatically updated or does it have to wait for the next scheduled WEP key propagation to be updated?



2. What is an access point? How do access points function? How do computers that communicate with the network through a wireless connection to an AP have their WEP keys updated? Would there simply be a PC card tray near all or most of the access points?

3. Are the WEP keys stored on the cards themselves? Are any modifications to the NIC cards necessary to accomplish this? If so, what are they? If not, how is the information stored and accessed on a standard NIC card?

4. Is the software implementation at each PC different from the prior art implementation at each PC? If so, is there any difference other than accessing a NIC for the WEP key? Please describe how the software functions providing a flowchart if possible.

**EXHIBIT D**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
APPLICATION FOR U.S. LETTERS PATENT

Title:

**METHOD AND APPARATUS FOR WEP KEY MANAGEMENT AND  
PROPAGATION IN A WIRELESS SYSTEM**

Inventor:

Doug Rollins

Dickstein Shapiro Morin &  
Oshinsky LLP  
2101 L Street, N.W.  
Washington, D.C. 20037  
(202) 785-9700

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR WEP KEY MANAGEMENT AND  
PROPAGATION IN A WIRELESS SYSTEM

5

FIELD OF THE INVENTION

[0001] The present invention relates to generally to network security, and, more particularly to a method and apparatus for Wired Equivalency Privacy key management and propagation in a wireless system.

BACKGROUND OF THE INVENTION

10

[0002] In a wired LAN, data transmissions are generally regarded as secure. Only those stations physically connected to the wire can receive the LAN traffic. For this reason, significant security precautions are generally not taken to protect the privacy of data transmissions within a LAN.

15

[0003] A network with wireless stations is not as secure. When data is transmitted to a wireless station, any station within range can eavesdrop on the transmission. The connection of a single wireless link (without any privacy protection) may seriously degrade the security level of the wired LAN.

20

[0004] Despite the security issues involved in implementing wireless stations, there are many advantages. A company can gain significant advantages by providing wireless connectivity to stations, such as, for example, automatic machinery or equipment that requires rapid deployment within a local area. The stations can be portable, hand-held or mounted on moving vehicles.

25

[0005] In an effort to preserve network security while using wireless stations, IEEE devised Wired Equivalency Privacy ("WEP"). WEP is a cryptographic confidentiality algorithm that can be used to provide data

confidentiality that is subjectively equivalent to the confidentiality of a wired local area network that does not use cryptographic techniques to enhance privacy.

[0006] An example of a wireless network is shown in Fig. 1. Wireless station 100 comprises a wireless network communications device 103, a microprocessor 101 and a data storage area 102. Wireless communications device 103 can be a wireless network interface card. Data storage area 102 stores the operating system and the support application for wireless station 100. An encryption key is stored within the support application.

[0007] Wired station 110 comprises a network communications device 113, a microprocessor 111 and a data storage area 112. Data storage area 112 stores the operating system and management application for wired station 110. Access point 120 is physically connected to wired station 110. Access point 120 is a bridge between the Ethernet network and the wireless network. These devices are well known in the art.

[0008] The process for updating encryption keys in a wireless network, such as that shown in Fig. 1, implementing WEP is shown in Fig. 2. The process begins when the network administrator selects a new encryption key at segment 200. IEEE 802.11x standard suggests a 40-bit or 128-bit encryption key, however, any convenient length may be used. The network administrator then propagates the new encryption key to access point 120. This can be accomplished one of two ways. If the vendor supplies a management application that supports automatic propagation to access points, then that may be used. If the vendor supplied management application does not provide the ability to automatically propagate new encryption keys to access points, the network administrator must manually enter the new encryption key at each access point. This entails writing the encryption key down and then manually entering it into the access point management application.

[0009] Once the encryption key at access point 120 is updated, no wireless network traffic can be decrypted by wireless station 100 until the encryption key at wireless station 100 is updated to match the updated encryption key at access point 120. In order to update the encryption key at wireless station 100 at segment 210, the network administrator must manually enter the new encryption key at wireless station 100. The encryption keys are stored in the software associated with wireless network communications device 103. As a result, the network administrator must physically access wireless station 100, start the operating system, open wireless communications device 103's support application and manually enter the WEP key at segment 210. This process must then be repeated for each wireless station.

[0010] Due to the cumbersome nature of manually changing the encryption keys at every wireless station, network administrators are reluctant to update encryption keys on a regular basis. When they do update the encryption key, it is a time-consuming task.

[0011] A quick, easy and secure method and apparatus for updating encryption keys in a wireless network is desirable.

#### SUMMARY OF THE INVENTION

[0012] The present invention mitigates the problems associated with the prior art and provides a unique method and apparatus for wired equivalency privacy key management and propagation in a wireless system.

[0013] In accordance with an exemplary embodiment of the present invention, an encryption key is stored in the wireless network communications device in each wireless station. When an encryption key is updated, a management station randomly generates a new encryption key and propagates it to all access points and PCMCIA card trays ("PC card tray"). Once the

encryption key is updated at each access point and the one or more PC card trays, the wireless network communications devices in each wireless station are removed and inserted into a PC card tray. The PC card trays update the encryption key stored in each wireless communications device. The wireless  
5 network communications devices are then reinserted into the wireless stations.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The above and other features and advantages of the invention will be more readily understood from the following detailed description of the invention which is provided in connection with the accompanying drawings.

10 [0015] Fig. 1 is a block diagram of a wireless network;

[0016] Fig. 2 is a flowchart of the process of updating the encryption keys in a wireless network in the prior art;

[0017] Fig. 3 is a flowchart of an exemplary embodiment of the present invention; and

15 [0018] Fig. 4 is a block diagram of a wireless network implementing an exemplary embodiment of the present invention.

#### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0019] In the following detailed description, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way  
20 of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to make and use the invention, and it is to be understood that structural changes may be made and equivalent structures substituted for those shown without departing from the spirit and scope of the present invention.

[0020] Fig. 3 shows an exemplary embodiment of the present invention implemented on the network shown in Fig. 4. Fig. 4 is identical to Fig. 1 except for the addition of a PCMCIA card tray 400 ("PC card tray"). PCMCIA (Personal Computer Memory Card International Association) established standards for memory and I/O devices for personal computers. PC card tray 400 has a plurality of slots each of which can receive an inserted wireless network communications device 103 that meets the PCMCIA standards. When wireless network communications device 103 is inserted into a slot of PC card tray 400, the PC card tray 400 accesses the encryption key stored in wireless communications device 103, erases the old encryption key and stores the updated encryption key.

[0021] Referring to Fig. 3, in an exemplary embodiment of the present invention, management station 110 checks the encryption key generation and propagation schedule at segment 300. If it is not a scheduled time to propagate a new encryption key, as determined at processing segment 305, management station 110 returns to segment 300. If management station 110 determines that it is time to propagate a new key according to the encryption key generation and propagation schedule at processing segment 305, management station 110 generates a new WEP key at segment 310.

[0022] The encryption key generation and propagation schedule can be determined by the network administrator. Encryption key updates can be set to take place on specific days at specific times, at specified intervals (e.g. every Monday), randomly or whenever a network administrator wants to change the encryption key. Once the network administrator determines how often to update the encryption keys, the network administrator can set the system to either automatically propagate the new encryption keys on schedule or to alert the network administrator to propagate the new encryption key.

[0023] Scheduled encryption key updates has several advantages. First, network security will not be compromised by extended periods of time using the same encryption key. Second, since management station 110 is generating the encryption key, rather than the network administrator, the encryption key is randomly generated. A randomly generated encryption key provides for greater security than a manually chosen one. Third, by verifying that the same encryption is not frequently used, network security is enhanced.

[0024] The system may also be set to prevent re-use of encryption keys. Thus, once a new encryption key is generated at segment 310, management station 110 verifies that the randomly generated encryption key is not identical to any of the  $k$  encryption keys that were previously used at processing segment 315. The number of previous encryption keys that each new encryption key is checked against can be set by the network administrator at management station 110. If the encryption key randomly generated at segment 310 matches one of the previous  $k$  encryption keys used, as determined at processing segment 315, that encryption key is discarded and management station 110 returns to segment 310 to randomly generate a new encryption key.

[0025] After management station 110 randomly generates an encryption key that is not identical to any of the previous  $k$  encryption keys, the new encryption key is propagated to all WEP-enabled devices at segment 320. Access points 120 and PC card trays 400 all store the new encryption key.

[0026] In a preferred embodiment of the present invention, there are two types of WEP capable devices. First, there are access points. Access points are bridges between the Ethernet network and the wireless network. These devices are well known in the art. Second, there are PC card trays. PC card trays are connected to the Ethernet and can have multiple PC cards inserted simultaneously. A crucial improvement of the present invention is that the



encryption key is stored in wireless communications device 103 rather than in data storage area 102. As a result, wireless communications device 103 can be removed from wireless station 100 and inserted into PC card tray 400 to be updated. Once wireless communications device 103 is inserted into PC card tray  
5 400, PC card tray 400 accesses the encryption key stored in wireless communications device 103, deletes the encryption key and stores the updated encryption key in wireless communications device 103. PC card trays can be connected to the Ethernet at any convenient location.

[0027] By allowing wireless communications device 103 to be updated  
10 by placing it in PC card tray 400, greater network security and reliability is achieved. First, since the encryption key is not written down and entered manually, there is no chance of the network administrator making an error while typing in the new encryption key. Second, since not even the network administrator knows what the encryption key is, the only way to obtain the  
15 encryption key is by gaining physical access to the network. Third, the network administrator does not have to physically access each wireless station 100. A technician, or even the user, can remove network communications device 103 from wireless station 100 and insert it into PC card tray 400. There can be many PC card trays placed at convenient locations so that the inconvenience is  
20 minimized.

[0028] If the device being updated is an access point, as determined at processing segment 325, then the encryption key is updated at segment 330. If the update is successful, as determined at processing segment 335, success is reported to management station 110 at segment 337. If the update is not  
25 successful, as determined at processing segment 335, failure is reported to management station 110 at segment 336. Management station 110 can then alert the network administrator of the failure so that the problem can be

corrected. If the device is not an access point, as determined at processing segment 325 and if the device is not a PC card tray 400, as determined a processing segment 340, the process ends.

[0029] If the device is a PC card tray 400, as determined at processing segment 340, the encryption key of the wireless communications device 103 in the first slot of PC card tray 400 is updated at segment 345. The encryption key stored in wireless communications device 103 can also be updated after the new encryption key has been propagated to the network by inserting it into PC card tray 400. If the encryption keys in all network communications devices 103 in PC card tray 400 have not been updated, as determined at processing segment 350, the network communications device 103 in the next slot of PC card tray 400 is updated at segment 360. If the encryption keys in all network communications devices 103 in PC card tray 400 have been updated, as determined at processing segment 350, success is reported to management station 110 at segment 355.

[0030] While the invention has been described with reference to exemplary embodiments various additions, deletions, substitutions, or other modifications may be made without departing from the spirit or scope of the invention. Accordingly, the invention is not to be considered as limited by the foregoing description, but is only limited by the scope of the appended claims.

What is claimed as new and desired to be protected by Letters Patent of the United States is:

1. A method of updating an encryption key in a wireless network, said method comprising:
  - 5 separating a communication device containing an encryption key from a wireless station of said network;
  - connecting said removed communications device to a wired portion of said network which contains an encryption key generator;
  - replacing an existing encryption key in said communications device with a  
10 new encryption key from said generator using a communication over said wired portion of said network; and
  - reconnecting said communications device containing said new encryption key with wireless station of said network.
- 15 2. A method as in claim 1, wherein said new encryption key is generated at user-defined intervals.
3. A method as in claim 1, wherein said new encryption key is generated on user-specified days.
4. A method as in claim 1, wherein said key generator generates a first new encryption key;  
20 compares said new encryption key to the previous ~~12~~ encryption keys used in said network; and

generates a second new encryption key if said first new encryption key matches any of said  $k$  previously used encryption keys.

5. A method as in claim 5, wherein  $k$  is a user-defined number of previously used encryption keys.

5 6. A method as in claim 1, wherein said network communication device is configured on a plug-in card and is connected to said network by inserting said network communications device into a PCMCIA card tray.

7. A method as in claim 6, wherein a plurality of network communications devices can be inserted into said PC card tray  
10 simultaneously.

8. A wireless network comprising:  
  
a wired station connected to a wired network, said wired station comprising:  
  
an encryption key generator for generating an encryption key; and  
  
a wired network communications device for transmitting said  
15 encryption key over said wired network;

a wireless station wirelessly connected to said wired network, said wireless station comprising:

a wireless network communications device containing an encryption key, said wireless network communications device being disconnected from said  
20 wireless station and connected to said wired network to receive and store as a new

encryption key, an encryption key transmitted over said wired network by said wired network communications device.

9. A wireless network as in claim 8, wherein said new encryption key is a randomly generated encryption key

5 10. A wireless network as in claim 8, wherein said new encryption key is generated by said generator and transmitted by said wired network communications device at user-defined intervals.

11. A wireless network as in claim 8, wherein when a newly generated encryption key is the same as one of k previously used encryption keys, said  
10 encryption key generator generates a new encryption key.

12. A wireless network as in claim 11, wherein k is a user-defined number.

13. A wireless network as in claim 8, further comprising a plurality of access points.

14. A wireless network as in claim 8, further comprising a PCMCIA card  
15 tray connected to said wired network, said wireless network communications device being connected to said wired network by insertion of said wireless network communications device into said PCMCIA card tray.

15. A wireless network wireless station comprising:  
  
a wireless network communications device for conducting wireless  
20 communications with a wired network, said wireless network communications device being removable from said station and storing an updateable encryption key used in

conducting encrypted wireless communications, said removable wireless network communications device being connectable to a wired network to receive and store a new encryption key.

16. A wireless station as in claim 15, wherein said wireless network  
5 communications device is adapted to be connected to a wired network by being insertable into a PCMCIA card tray connected to said wired network.

17. A wireless network communications device comprising:  
  
a removable network card adapted to be connected and disconnected from a card interface;  
  
10 a wireless network communications interface provided on said network card which stores an updateable encryption key for use in conducting encrypted wireless network communications, said encryption key being updateable when said card is connected to a card interface which supplies a new encryption key.

18. A wireless network communications card as in claim 17, wherein said  
15 card interface for providing a new encryption key is a PCMCIA card interface.

19. A wireless network communications card as in claim 18, wherein said PCMCIA card interface is provided at a PCMCIA card tray.

20. An encryption key programming system comprising:  
  
an encryption key generator connected to a wired network;  
  
20 a programming device connected to said wired network for receiving over a wire connection an encryption key from said generator, said programming device

being adapted to receive a wireless network communications device and storing said received encryption key therein.

21. An encryption key programming system as in claim 20, wherein said encryption key generator generates a random encryption key.

5 22. An encryption key programming system as in claim 20, wherein said encryption key generator generates a new encryption key at user-defined intervals.

23. An encryption key programming system as in claim 20, wherein said encryption key generator generates a new encryption key on user-specified days.  
10

24. An encryption key programming system as in claim 20, wherein said encryption key generator generates a first new encryption, compares said new encryption key to the previous  $k$  encryption keys used in said network and generates a second new encryption key if said first new encryption key matches any of said  $k$  previously used encryption keys;  
15

25. An encryption key programming system as in claim 20, wherein  $k$  is a user-defined number of previously used encryption keys.

26. An encryption key programming system as in claim 20, further comprising a PCMCIA card tray connected to said programming device, said wireless communications device being received by said programming device  
20

by insertion of said wireless communications device into said PCMCIA card  
tray.



ABSTRACT

A method and apparatus for WEP key management and propagation in a wireless system is disclosed. Encryption keys at each wireless station are stored on a wireless network communication devices at each wireless station. For encryption key is updating, a management station randomly generates a new encryption key and propagates it to a wired device in a wired network which can receive a wireless network communications device and update its encryption key.

## **EXHIBIT E**

D I C K S T E I N   S H A P I R O   M O R I N   &   O S H I N S K Y   L L P

2101 L Street NW • Washington, DC 20037-1526

Tel (202) 785-9700 • Fax (202) 887-0689

Writer's Direct Dial: (202) 828-2232

Writer's EMail: [DAmicoT@DSMO.com](mailto:DAmicoT@DSMO.com)

October 22, 2001

Ms. Stacy L. Summers  
Micron Technology, Inc.  
8000 S. Federal Way  
Boise, Idaho 83707-0006


**PRIVILEGED AND CONFIDENTIAL:**  
**ATTORNEY-CLIENT COMMUNICATION**

Re:        U.S. Patent Application  
            Application No.: Not Yet Assigned  
            Title: METHOD AND APPARATUS FOR WEP KEY MANAGEMENT  
                         AND PROPAGATION IN A WIRELESS SYSTEM  
            Inventor: Doug Rollins  
            Our Reference: M4065.0486/P486

Dear Stacy:

Enclosed please find three copies of a first draft of a patent application for Micron's invention entitled "Method and Apparatus for WEP Key Management and Propagation in a Wireless System." This draft has been prepared based upon the original invention submission.

Please have the inventor review this draft to ensure that it completely and accurately describes the invention.



## EXHIBIT F

**Borchers, Julia**

---

**From:** Rozar, Maxine  
**Sent:** Friday, November 02, 2001 8:02 AM  
**To:** Kaplan, Adam; Borchers, Julia  
**Subject:** FW: 70-0586 (.0486)

Please send papers per Stacy's request below.

-----Original Message-----

**From:** slsummers [mailto:slsummers@micron.com]  
**Sent:** Thursday, November 01, 2001 6:07 PM  
**To:** 'rozarm@dsmo.com'  
**Cc:** 'damicot@dsmo.com'  
**Subject:** 70-0586 (.0486)

Max,

Could you please have the secretary working with the above reference send me a copy of the signature papers for the inventor to execute?

Thanks, Stacy

## **EXHIBITG**

DICKSTEIN SHAPIRO MORIN & OSHINSKY LLP

2101 L Street NW • Washington, DC 20037-1526

Tel (202) 785-9700 • Fax (202) 887-0689

Writer's Direct Dial: (202) 828-2232

Writer's EMail: DAmicoT@DSMO.com

November 7, 2001

Ms. Stacy L. Summers  
Micron Technology, Inc.  
8000 S. Federal Way  
Boise, Idaho 83707-0006

**PRIVILEGED AND CONFIDENTIAL:**  
**ATTORNEY-CLIENT COMMUNICATION**

Re: U.S. Patent Application  
Title: METHOD AND APPARATUS FOR WEP KEY MANAGEMENT  
AND PROPAGATION IN A WIRELESS SYSTEM  
Inventor: Doug Rollins  
Your Reference: 70-0586  
Our Reference: M4065.0486/P486

Dear Stacy:

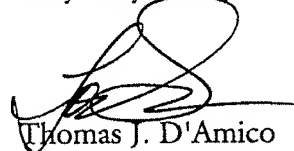
Enclosed please find three copies of a signature draft of a patent application for Micron's invention entitled "Method and Apparatus for WEP Key Management and Propagation in a Wireless System."

Please have the inventor review the signature draft to ensure that it completely and accurately describes the invention. If in the final review, they note the need for any minor revisions, please contact us.

Also enclosed are the Declaration for Patent Application, Assignment and Agreement, and Power of Attorney by Assignee and Certificate by Assignee Under 37 C.F.R. § 3.73(b) forms. Please have the application executed and returned to us at your earliest convenience. We will file it as soon as we receive it.

If you have any questions, please do not hesitate to call.

Very truly yours,



Thomas J. D'Amico

TJD/ASK/jlb  
Enclosures

1177 Avenue of the Americas • 41st Floor • New York, New York 10036-2714

Tel (212) 835-1400 • Fax (212) 997-9880

[www.legalinnovators.com](http://www.legalinnovators.com)

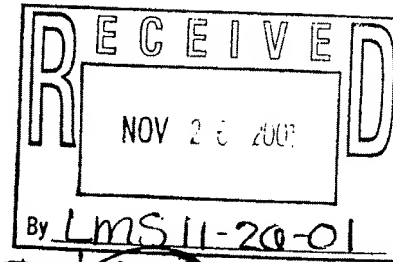


## EXHIBIT H

November 21, 2001

Micron Technology, Inc.  
8000 S. Federal Way  
P.O. Box 9  
Boise, ID 83707-0009  
208-368-4000

Tom D'Amico  
Dickstein, Shapiro, Morin  
& Oshinsky  
2101 L Street N.W.  
Washington, D.C. 20037



Re: Micron Docket # 70-0586  
Your Ref. # M4065.0486 /p486

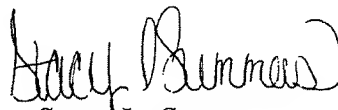
Dear Tom:

Please find enclosed the following signature papers, which have been signed by the inventors and are ready to be filed with the Patent Office:

- 1) Declaration;
- 2) Assignment; and
- 3) Power of Attorney.

Please fax me a copy of the transmittal letter when this case is filed with the PTO. Feel free to let me know if you have any questions.

Very truly yours,

  
Stacy L. Summers  
Patent Assistant

Phone: 208/368-4591  
Fax: 208/368-5606

*The future of memory*